5

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/680,294	10/08/2003	Masato Yamamichi	2003_1411A	4208

513 7590 01/29/2007
WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
KOEMPEL THOMAS, BEATRICE L	
ART UNIT	PAPER NUMBER
2132	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/29/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/680,294	**Applicant(s)** YAMAMICHI ET AL.	
	Examiner Bea Koempel-Thomas	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 08 October 2003.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *See Continuation Sheet*.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

Continuation of Attachment(s) 3). Information Disclosure Statement(s) (PTO/SB/08), Paper No(s)/Mail Date :9 January 2004 and 30 March 2004.

DETAILED ACTION

1. Claims 1-35 are pending in this application and presented for examination.

Objections

Information Disclosure Statement

2. The information disclosure statement filed 30 March 2004, fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

Specification

3. The use of the trademark NTRU has been noted in this application (page 1 line 8, et seq.). It should be capitalized wherever it appears or include a proper trademark symbol, such as ™ or © following the word **and be accompanied by the generic terminology**.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner that might adversely affect their validity as trademarks. Appropriate correction is requested.

4. The listing of references in the specification (page 1 lines 20-22, et seq.) is not a proper information disclosure statement. 37 CFR 1.98(b) requires a list of all patents, publications, or other information submitted for consideration by the Office, and MPEP § 609.04(a) states, "the list may not be incorporated into the specification but must be submitted in a separate paper."

Therefore, unless the references have been cited by the examiner on form PTO-892, they have not been considered.

5. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code (pages 2-3 lines 32-1). Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. See MPEP § 608.01.

6. Examiner notes incorporation of essential material in the specification by reference to the foreign priority application without an accurate English language translation of the certified copy. If the material is relied upon to overcome any objection, rejection, or other requirement imposed by the Office, the applicant will be required to amend the disclosure to include the material incorporated by reference. Such amendment must be accompanied by a statement executed by the applicant, or a practitioner representing the applicant, stating that the material being inserted is the material previously incorporated by reference and that the amendment contains no new matter. 37 CFR 1.57(f).

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

8. Claims 32-35 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claims 32 and 33 could reasonably be drawn to functional descriptive material, per se, i.e., "program" may be taken to mean software alone, and as such, claims 32 and 33, would be directed to non-statutory subject matter. The specification does not preclude this interpretation. Claims 34 and 35 could reasonably be drawn to non-functional

descriptive material, per se, i.e., "an encryption program . . . is recorded" may be taken to mean a program listing recorded on a computer-readable storage medium without any functional interrelationship, and as such, claims 34-35, would be directed to non-statutory subject matter. The specification does not preclude this interpretation. Further, claims 32-35 do not necessarily transform a physical object to a different state or thing nor produce a useful, concrete and tangible result.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 2, 4, 7, 11, 19, 20, 27, 30, and claims dependent thereon are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The limitation "as time goes by" fails to apprise one of ordinary skill in the art the requisite time period applicant is claiming.

Claim Rejections - 35 USC § 102

11. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

12. **Claims 1, 2, 7, 13, 26, 27, 32, and 34 are rejected under 35 U.S.C. 102(b) as being anticipated by DeBellis et al. U.S. Patent No. 6,104,810 (hereinafter DeBellis).**

13. **Regarding claim 1:** DeBellis discloses an encryption apparatus for generating an encrypted text by encrypting a plaintext, comprising:

a storage unit operable to store an encryption key and a parameter which is adapted to a decryption apparatus and changes a probability of decryption error in decrypting the encrypted text (col. 5 lines 40-51);

an encryption unit operable to generate the encrypted text from the plaintext, using the encryption key and the parameter stored in the storage unit, according to an encryption algorithm which changes the probability of the decryption error in decrypting the encrypted text depending on a value of the parameter (col. 12 lines 15-26); and

an updating unit operable to update the parameter stored in the storage unit (col. 5 lines 40-51).

14. **Regarding claims 26, 32 and 34:** DeBellis discloses an encryption method, program, and program storage device, respectively, for generating an encrypted text by encrypting a plaintext, comprising:

an encrypted text generating step of generating the encrypted text from the plaintext, using the encryption key and a parameter, according to an encryption algorithm which changes the probability of the decryption error in decrypting the encrypted text depending on a value of the parameter adapted to a decryption apparatus (col. 12 lines 15-26); and

an updating step of updating the parameter (col. 5 lines 40-51).

15. **Regarding claim 2:** DeBellis discloses that the updating unit updates the parameter stored in the storage unit, as time goes by (col. 5 lines 40-51).

16. **Regarding claims 7 and 27:** DeBellis discloses that the updating unit updates the parameter so that the probability of the decryption error in decrypting the encrypted text increases as time goes by (col. 5 lines 15-27).

17. **Regarding claim 13:** DeBellis discloses an encryption key updating unit operable to receive, from the decryption apparatus, a request to update the encryption key, and update the encryption key in response to the updating request (col. 7 lines 26-32); and a parameter initialization unit operable to receive, from the decryption unit, a request to update the parameter (col. 5 lines 28-39), and set, in response to the initialization request, a value of the parameter to an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value (col. 12 lines 15-26).

18. **Claims 14, 17, 31, 33, and 35 are rejected under 35 U.S.C. 102(b) as being anticipated by Geiringer, PCT Publication No. WO 01/93013 A1 (hereinafter Geiringer).**

19. **Regarding claim 14:** Geiringer discloses a decryption apparatus for decrypting an encrypted text, comprising:

a decryption unit operable to generate a decrypted text using a decryption key, from the encrypted text generated according to an encryption algorithm which changes a probability of decryption error in decrypting the encrypted text depending on a value of a parameter (page 22 lines 15-18);

a judgment unit operable to judge whether or not the decrypted text is obtained correctly (page 27 lines 25-28);

a decryption key updating request unit operable to request an encryption apparatus to update the decryption key, according to a result of the judgment made by the judgment unit (page 28 lines 12-20); and

a parameter initialization request unit operable to request the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of the decryption error in decrypting the encrypted text to a value less than or equal to a predetermined value (page 28 lines 18-20).

20. **Regarding claim 17:** Geiringer discloses that the judgment unit judges that the decrypted text is not obtained correctly, when the probability of the decryption error in decrypting the encrypted text during a predetermined period of time exceeds a predetermined threshold (page 28 lines 22-28).

21. **Regarding claims 31, 33, and 35:** Geiringer discloses a decryption method, program, and program storage device, respectively, for decrypting an encrypted text, comprising:

a decryption step of generating a decrypted text using a decryption key, from the encrypted text generated according to an encryption algorithm which changes a probability of decryption error in decrypting the encrypted text depending on a value of a parameter (page 22 lines 15-18);

a judgment step of judging whether or not the decrypted text is obtained correctly (page 27 lines 25-28);

an updating request step of requesting an encryption apparatus to update the decryption key, according to a result of the judgment in the judgment step (page 28 lines 12-20); and

an initialization request step of requesting the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of decryption error to a value less than or equal to a predetermined value, according to the result of the judgment in the judgment step (page 28 lines 18-20).

Claim Rejections - 35 USC § 103

22. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

23. **Claims 3-5, 10, 11, 18-20, 25, 29, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeBellis in view of Geiringer.**

24. **Regarding claim 18:** DeBellis discloses an encryption system comprising an encryption apparatus (col. 6 line 39) including:

a storage unit operable to store an encryption key and a parameter which is adapted to a decryption apparatus and changes a probability of decryption error in decrypting the encrypted text (col. 5 lines 40-51);

an encryption unit operable to generate the encrypted text from the plaintext, using the encryption key and the parameter stored in the storage unit, according to an encryption algorithm which changes the probability of the decryption error in decrypting the encrypted text depending on a value of the parameter (col. 12 lines 15-26); and

an updating unit operable to update the parameter stored in the storage unit (col. 5 lines 40-51).

DeBellis does not disclose a decryption apparatus for generating a decrypted text by decrypting the encrypted text, and the decryption apparatus including: a decryption unit operable to generate a decrypted text from the encrypted text using a decryption key; a decryption key updating request unit operable to request the encryption apparatus to update the decryption key; and a parameter initialization request unit operable to request the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value.

Geiringer discloses an encryption system (page 22 lines 15-18) comprising a decryption apparatus for generating a decrypted text by decrypting the encrypted text, the decryption apparatus (page 26 line 28) including:

a decryption unit operable to generate a decrypted text from the encrypted text using a decryption key (page 22 lines 15-18);

a decryption key updating request unit operable to request the encryption apparatus to update the decryption key (page 28 lines 12-20); and

a parameter initialization request unit operable to request the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value (page 28 lines 18-20).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the encryption system of DeBellis by the decryption components of an encryption system as taught by Geiringer in order to create an efficient and secure encryption system based on mixing seeds (*see* Geiringer page 16 lines 24-25).

25. **Regarding claims 3, 10, 23, and 29:** DeBellis does not disclose that the encryption unit generates the encrypted text using the encryption algorithm based on an NTRU encryption method. Geiringer discloses that the encryption unit generates the encrypted text using the encryption algorithm based on an NTRU encryption method (page 1 lines 7-11).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the encryption system of DeBellis for use of the NTRU algorithm as taught by Geiringer in order to create an efficient and secure encryption system based on mixing seeds (*see* Geiringer page 16 lines 24-25).

26. **Regarding claims 4, 11 and 30:** DeBellis discloses a parameter stored in a storage unit and an updating unit operating as time goes by (col. 5 lines 40-51).

DeBellis does not disclose that the parameter indicates the number of terms whose coefficients indicate 1 in a random number polynomial based on the NTRU encryption method or that the number of terms whose coefficients indicate 1 in the random number polynomial is increased. Geiringer discloses that the parameter indicates the number of terms whose coefficients indicate 1 in a random number polynomial (page 22 lines 5-12) based on the NTRU encryption method (page 1 lines 7-11) and that the number of terms whose coefficients indicate 1 in the random number polynomial is increased (page 3 lines 14-18).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the encryption system of DeBellis for use of the NTRU algorithm as taught by Geiringer in order to create an efficient and secure encryption system based on mixing seeds (*see* Geiringer page 16 lines 24-25).

27. **Regarding claim 5:** DeBellis discloses an encryption key updating unit operable to receive, from the decryption apparatus, a request to update the encryption key and update the encryption key in response to the updating request (col. 7 lines 26-32); and an initialization unit (col. 5 lines 28-39) and setting in response to the updating request, an initial value which decreases the probability of the decryption error to a value less than or equal to a predetermined value (col. 12 lines 15-26).

DeBellis does not disclose updating or setting the number of the terms whose coefficients indicate 1 in the random number polynomial.

Geiringer discloses updating or setting the number of the terms whose coefficients indicate 1 in the random number polynomial (page 22 lines 5-12).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the encryption system of DeBellis for use of the NTRU algorithm as taught by Geiringer in order to create an efficient and secure encryption system based on mixing seeds (*see* Geiringer page 16 lines 24-25).

28. **Regarding claim 19:** DeBellis discloses that the updating unit updates the parameter stored in the storage unit, as time goes by (col. 5 lines 40-51).

29. **Regarding claim 20:** Claim 20 is rejected for the same reasons as claims 3 and 4, above.

30. **Regarding claim 25:** DeBellis does not disclose that the decryption apparatus further includes a judgment unit operable to judge whether or not the decrypted text is obtained correctly, the decryption key updating request unit instructs the encryption apparatus to update the decryption key, according to a result of the judgment made by the judgment unit, and the parameter initialization request unit instructs the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of decryption error to a value less than or equal to a predetermined value, according to the result of the judgment made by the judgment unit.

Geiringer discloses that the decryption apparatus further includes a judgment unit operable to judge whether or not the decrypted text is obtained correctly (page 27 lines 25-28),

the decryption key updating request unit instructs the encryption apparatus to update the decryption key, according to a result of the judgment made by the judgment unit (page 28 lines 12-20), and

the parameter initialization request unit instructs the encryption apparatus to change the value of the parameter to an initial value which decreases the probability of decryption error to a value less than or equal to a predetermined value, according to the result of the judgment made by the judgment unit (page 28 lines 18-20).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the encryption system of DeBellis by the decryption apparatus taught by Geiringer in order to create an efficient and secure encryption system based on mixing seeds (*see* Geiringer page 16 lines 24-25).

31. **Claims 8, 9, 22, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeBellis in view of Nishio et al. U.S. Patent No. 5,848,154 (hereinafter Nishio).**

32. **Regarding claims 8 and 22:** DeBellis discloses an updating unit as indicated regarding claim 1. DeBellis does not disclose that the updating unit updates the parameter stored in the storage unit according to the number of times the encryption unit performs encryption.

Nishio discloses that the updating unit updates the parameter stored in the storage unit according to the number of times the encryption unit performs encryption (col. 3 lines 22-35).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the encryption system of DeBellis by the quantity management system taught by Nishio for the benefit of managing the number of times encryption is performed (*see* Nishio col. 1 lines 50-62).

33. **Regarding claims 9 and 28:** DeBellis discloses an updating unit as indicated regarding claim 1. DeBellis does not disclose that the updating unit updates the parameter so that the probability of the decryption error in decrypting the encrypted text increases according to an increase in the number of times the encryption apparatus performs encryption.

Nishio discloses that the updating unit updates the parameter so that the probability of the decryption error in decrypting the encrypted text increases according to an increase in the number of times the encryption apparatus performs encryption (col. 3 lines 22-45).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the encryption system of DeBellis by the quantity management system taught by Nishio for the benefit of managing the number of times encryption is performed (*see* Nishio col. 1 lines 50-62).

34. **Claims 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Geiringer in view of Nishio.**

35. **Regarding claim 15:** Geiringer discloses a decryption apparatus including a decryption key updating request unit and the parameter initialization request unit send respectively, to the encryption apparatus, a request to update the decryption key and a request to initialize the parameter as indicated regarding claim 14. Geiringer does not disclose a request to pay a predetermined amount.

Nishio discloses a request to pay a predetermined amount (col. 3 lines 22-35).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the decryption apparatus of Geiringer by the quantity use management system taught by Nishio for the benefit of managing the number of times decryption is performed (*see* Nishio col. 1 lines 50-62).

36. **Regarding claim 16:** Geiringer discloses a judgment unit that judges that the decrypted text is not obtained correctly, when the probability of the decryption error in decrypting the encrypted text during a predetermined period of time exceeds a predetermined threshold (page 28 cines 22-28).

37. **Claims 6, 21 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeBellis in view of Geiringer, further in view of Nishio.**

38. **Regarding claim 6:** DeBellis and Geiringer disclose an encryption apparatus, wherein the initialization unit sets the number of the terms whose coefficients indicate 1 in the random number polynomial to an initial value as indicated regarding claim 5, above. DeBellis and Geiringer do not disclose setting the number when the decryption apparatus has paid a predetermined amount.

Nishio discloses setting the number when the decryption apparatus has paid a predetermined amount (col. 3 lines 22-35).

Therefore, it would have been obvious to one skilled in the art at the time of the invention to modify the combination of DeBellis and Geiringer by the quantity use management system taught by Nishio for the benefit of managing payments for performing decryption (*see* Nishio col. 1 lines 50-62).

39. **Regarding claim 21:** the combination of DeBellis and Geiringer discloses an encryption system, wherein the decryption key updating request unit and the parameter initialization request

unit respectively send, to the encryption apparatus, a request to update the decryption key and a request to initialize the parameter as indicated regarding claim 20, above.

DeBellis further discloses that the encryption apparatus includes: a decryption key updating unit operable to receive, from the decryption apparatus, the request to update the decryption key, and update the decryption key in response to the updating request col. 7 lines 26-32).

DeBellis does not disclose an initialization unit operable to receive the request to initialize the parameter from the decryption apparatus, and set, in response to the initialization request, the number of the terms whose coefficients indicate 1 in the random number polynomial to an initial value which decreases a probability of decryption error to a value less than or equal to a predetermined value.

Geiringer discloses an initialization unit (page 3 lines 14-18) operable to receive the request to initialize the parameter from the decryption apparatus, and set, in response to the initialization request, the number of the terms whose coefficients indicate 1 in the random number polynomial to an initial value which decreases a probability of decryption error to a value less than or equal to a predetermined value (page 28 lines 18-20).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the encryption system of DeBellis by the decryption apparatus taught by Geiringer in order to create an efficient and secure encryption system based on mixing seeds (*see* Geiringer page 16 lines 24-25).

Neither DeBellis nor Geiringer disclose a system responsive to payment of a predetermined amount.

Nishio discloses a system responsive to payment of a predetermined amount (col. 3 lines 22-35).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the combination of DeBellis and Geiringer by the quantity use management system taught by Nishio for the benefit of managing payments for an encryption system (*see* Nishio col. 1 lines 50-62).

40. **Regarding claim 24:** Claim 24 is rejected for the same reasons as claims 4 and 21, above.

41. **Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over DeBellis in view of Geiringer, further in view of Whyte, "Analysis of NTRUEncrypt Paddings, STRONG security that fits everywhere," NTRU, August 2002 (hereinafter Whyte).**
Regarding claim 24: the combination of DeBellis and Geiringer discloses an encryption apparatus wherein the encryption unit generates the encrypted text using the encryption algorithm used for the NTRU encryption method as indicated regarding claim 10, above.

Neither DeBellis nor Geiringer disclose that the algorithm used for the NTRU encryption method is based on an EESS (Efficient Embedded Security Standard) method.

Whyte discloses that the algorithm used for the NTRU encryption method is based on an EESS (Efficient Embedded Security Standard) method (Whyte page 7 line 2).

Therefore it would have been obvious to one skilled in the art at the time of the invention to modify the combination of DeBellis and Geiringer by the EESS compatible NTRU encryption method as taught by Whyte in order to construct a standards compatible system (Whyte page 7 line 2).

Conclusion

42. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure is:

- Ruehle, U.S. Patent Application Publication No. 2003/0059045 A1, regarding a has-based pseudo-random number generator.
- Hoffstein et al., U.S. Patent No. 7,031,468 B2, regarding a speed enhanced cryptographic method and apparatus.
- Schell et al., U.S. Patent Application Publication No. 2003/0061483 A1, regarding a nested strong loader apparatus and method.
- Wenocur et al., U.S. Patent Application Publication No. 2002/0165912 A1, regarding a system and method for issuing a secure certificate.
- Yokota et al., U.S. Patent Application Publication No. 2003/0021421 A1, regarding a method of producing a decrypting apparatus having a cryptographic device.

Please direct any inquiry concerning this communication or earlier communications from the examiner to Bea Koempel-Thomas whose telephone number is 571-270-1252. The examiner can normally be reached on Monday - Friday; 0830 - 1700.

If attempts to reach the examiner by telephone are unsuccessful, please contact the examiner's supervisor, Gilberto Barron, at 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Bea Koempel-Thomas, Esq.
Patent Examiner
AU 2132

1/23/2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100